Expanding the view on Offensive Cyber Operations

Emil Larsson

Faculty of Health, Science and Technology

Computer Science

LICENTIATE THESIS | Karlstad University Studies | 2025:20

Expanding the view on Offensive Cyber Operations

Emil Larsson

LICENTIATE THESIS | Karlstad University Studies | 2025:20

Expanding the view on Offensive Cyber Operations

Emil Larsson

LICENTIATE THESIS

Karlstad University Studies | 2025:20

urn:nbn:se:kau:diva-103876

ISSN 1403-8099

ISBN 978-91-7867-572-2 (print)

ISBN 978-91-7867-573-9 (pdf)

https://doi.org/10.59217/bdrf5749

© The author

Distribution:
Karlstad University
Faculty of Health, Science and Technology
Department of Mathematics and Computer Science
SE-651 88 Karlstad, Sweden
+46 54 700 10 00

Print: Universitetstryckeriet, Karlstad 2025

WWW.KAU.SE

Abstract

Society relies upon the internet, a globally interconnected collection of networked information systems. These systems are imperfectly designed and implemented with critical flaws and vulnerabilities. Criminal hackers attack these shortcomings for financial gains, but there are also compelling reasons for states and state-sponsored groups to act in and through cyberspace. While state-sponsored cyberattacks can be both permissible and effective, they commonly have unintended effects: cyber collateral damage.

Most offensive cyber operations are conducted below the threshold of force recognized in international law and do not qualify for a military response. This means that they can be used both for clandestine sabotage, for intelligence gathering, and to implant vulnerabilities in preparation for larger-scale attacks in the future. These activities have caused considerable harm beyond their intended targets. Such collateral effects have been seen in some of the most infamous and costly cyberattacks, such as the 2010 Stuxnet attack, the 2017 NotPetya attack, and the 2022 attack on ViaSat as part of the invasion of Ukraine.

An under-investigated metric when analyzing the impact of cyber operations is their economic cost, both in terms of production and (especially) in their collateral cost to society. The economic cost is also subject to considerable externalization in the planning of cyber operations. This thesis thus investigates the balance between the operational effects of cyber operations and their collateral costs; the cost/benefit dilemma of offensive cyber operations. It does so by considering the potential benefit of high-impact cyberattacks, e.g. supply chain vulnerability implantation against hardened targets, and by using econometric methods to calculate the cost of collateral damage engendered when cyberspace is used as a domain of warfare. In doing so, it provides the first quantitative comparison of military utility to civilian harm in a cyber context. Although cyberattacks have long been considered a central component in asymmetric warfare, the thesis presents a bottom-up analysis which shows that the economic damage caused by cyberattacks in the Russo-Ukrainian conflict 2014-2021 is an insignificant part of the Ukrainian GDP.

Finally, the thesis argues that the full cost of attacks should be measured and included in models for collateral damage estimation. Such

estimates should be included into national cyber doctrines to minimize unintended effects and ensure efficient and appropriate use of cyber capabilities.

Keywords: cybersecurity, cyber warfare, collateral damage, structured literature review, applied econometrics

Ett utökat perspektiv på offensiva cyberoperationer

Sammanfattning

Det moderna samhället bygger på internet, ett globalt datornätverk som utgörs av sammankopplade informationssystem. Dessa system kan aldrig vara helt säkra utan lider av kritiska brister och sårbarheter. Kriminella hackare attackerar dessa brister för ekonomisk vinning, men det finns också skäl för stater och statligt sponsrade grupper att agera i och genom cyberrymden. Även om statligt sponsrade cyberattacker kan vara både tillåtna och effektiva ger de oavsiktliga effekter, så kallade sidoskador.

De flesta offensiva cyberoperationer utförs under den tröskel för angrepp som erkänns i internationell rätt, och kan därför inte besvaras med väpnad konflikt. Detta innebär att cyberoperationer kan användas både för sabotage, för underrättelseinhämtning, och för att plantera in sårbarheter som förberedelser för framtida attacker. Dessa aktiviteter har orsakat avsevärda sidoskador utöver de avsedda målen. Sidoskadorna har särskilt uppmärksammats vid de mest ökända och kostsamma cyberattackerna som Stuxnet år 2010, Notpetya 2017, och vid 2022 års attack mot ViaSat i samband med invasionen av Ukraina. Vid analyser av cyberoperationers effekt mäts sällan deras ekonomiska kostnad, varken i termer av produktionskostnaden eller i termer av den ekonomiska skada de åsamkar samhället. Den ekonomiska kostnaden är också föremål för betydande externalisering i planeringen av cyberoperationer. Denna avhandling undersöker därför balansen mellan de operativa effekterna av cyberoperationer och deras totala kostnader, det vill säga avvägningen mellan kostnad och nytta vid planering och utförande av offensiva cyberoperationer. Avhandlingen gör det genom att undersöka den potentiella nyttan av cyberattacker med stor effekt, t.ex. implantering av sårbarheter i försörjningskedjan mot härdade mål, och genom att använda ekonometriska metoder för att beräkna kostnaden för de sidoskador som uppstår när cyberrymden används som en domän för krigföring. Avhandlingen ger därmed den första kvantitativa jämförelsen av militär nytta och civil skada i ett cybersammanhang. Även om cyberattacker länge har ansetts vara en central komponent i asymmetrisk krigföring, presenterar avhandlingen en databaserad analys som visar att de ekono-

miska kostnaderna för cyberattackerna i den rysk-ukrainska konflikten 2014-2021 var små jämfört med Ukrainas BNP.
Slutligen argumenterar avhandlingen för att cyberattackernas fullständiga kostnad bör mätas och inkluderas i modeller för uppskattning av sidoskador. Sådana uppskattningar bör därefter inkluderas i nationella cyberdoktriner för att minimera oavsiktliga effekter och säkerställa en effektiv och lämplig användning av cyberförmåga.

Nyckelord: cybersäkerhet, cyberkrigföring, sidoskador, strukturerad litteraturöversikt, tillämpad ekonometri

Acknowledgments

Not everyone gets the privilege of being paid to find things out. Thus, I would like to gratefully acknowledge the financial support provided by the Knowledge Foundation (KK-Stiftelsen) and the generous permission of the Assemblin Caverion Group to freely mix work and research. Each was a necessary, but not sufficient, precondition for this project.
I would also like to thank my three supervisors. Johan Sigholm has been the best imaginable companion on this journey from the start. Meiko Jensen brought a smile and a laugh to every meeting. Hans Liwång protected me and the project from outside demands.
Thank you also to Simone Fischer-Hübner for making the Swedish Industrial Graduate School - Cyber a reality.
I received proofreading assistance, quality assurance, and valuable comments from Sarah Backman, Vera van Zoest, Sebastian Herold, and Jörgen Hansson.

Finally, the greatest love and gratitude go to my family for supporting me in this endeavor.

Stockholm, March 2025 Emil Larsson

List of Appended Papers

I. **Emil Larsson**. Collateral Damage from Offensive Cyber Operations – a Systematic Literature Review. In review for publication.

II. Johan Sigholm, **Emil Larsson**. Determining the Utility of Cyber Vulnerability Implantation - The Heartbleed Bug as a Cyber Operation. In: 2014 IEEE Military Communications Conference (MILCOM), pp. 110-116. IEEE, 2014.

III. **Emil Larsson**, Johan Sigholm. Papering over the cracks: The effects of introducing best practices on the web security ecosystem. In: 2016 International Conference on Information Networking (ICOIN), pp. 1-6. IEEE, 2016.

IV. Johan Sigholm, **Emil Larsson**. Cyber Vulnerability Implantation Revisited. In: 2021 IEEE Military Communications Conference (MILCOM), pp. 464-469. IEEE, 2021.

V. **Emil Larsson**, Johan Sigholm. Towards econometric estimation of the societal cost of cyber conflict. Procedia Computer Science 246, pp. 2535-2644. Springer Verlag, 2024.

Comments on my Participation

Paper I I am the sole author of the paper.

Paper II Johan Sigholm and I co-authored the paper. I performed all the data entry and preliminary analysis. I also constructed and validated the mathematical model of vulnerability propagation speed. Both co-authors helped in writing and revising the final article. I presented the paper at the scientific conference.

Paper III Johan Sigholm and I co-authored the paper. I proposed the relevant contribution to this thesis, the proposed model extension. Both co-authors helped in writing and revising the final article. I presented the paper at the scientific conference.

Paper IV Johan Sigholm and I co-authored the paper. This paper revisits the predictions made in Paper I and verifies that they did in fact occur as predicted. I did all the data entry and preliminary analysis. I also re-calculated, extended and validated the mathematical model of vulnerability propagation speed. Both co-authors helped in writing and revising the final article. I presented the paper at the scientific conference.

Paper V I am the main author of the paper. I proposed the research question, located, and adapted the model, and entered and analyzed the data. Both co-authors helped in writing as well as in revising the final article. I presented the paper at the scientific conference.

Contents

Introductory summary

1 Introduction

The development of networked information systems has greatly improved the productivity of modern society. These systems support essential services, such as communications, finance, energy management, and healthcare. Ensuring the security and safety of information systems is a key priority for companies and government institutions alike. Within the field of IT and information security, it is common to encounter incidents—unexpected events that disrupt operational processes [1]. These can be caused not just by poorly developed systems, faulty processes, or human error, but also by malicious and direct action across computer networks: cyberattacks. In 2021, companies spent some $150 billion on IT security globally, and still suffered cyberattack damages several times greater [2]. Most of these attacks are conducted by criminals for the purpose of monetary gain, but an increasing number of states and state-affiliated actors are also leveraging capabilities to operate in cyberspace [3].

When states operate in cyberspace, the operations can be conducted under different auspices including law enforcement, national security, or by the military forces. Distinct practical and legal frameworks exist to regulate each of these areas. In practice, cyber operations are often conducted under a veil of secrecy. Even operations which are discovered can be difficult to attribute to some specific state actor with any reasonable amount of certainty. These characteristics mean that state-backed cyberattacks, or offensive cyber operations, show an alarming but clear tendency towards civilian harm [4]. This harm occurs either because of callous disregard of unintended consequences, through the use of crypto-ransomware and other criminal covers as deception, through the destruction of information and systems to cover the tracks and confuse forensic investigators, or by directly attacking civilian infrastructure [5]. In addition, states and state-backed actors often have access to money, manpower, and technical resources, and can spend longer than criminals and other hackers when planning and executing a cyber operation. As a result, while state-backed cyberattacks constitute a clear minority of attacks, they are often dis-

proportionally destructive [6]. The costliest cyberattack known to date, generally referred to as NotPetya, occurred in 2017 and was conducted as part of the Russo-Ukrainian war. It caused damages in the billions of dollars, with the most heavily affected firm, pharmaceutical giant Merck & Co, eventually receiving a $1.4B insurance payout [7].

Many organizations which operate critical infrastructure such as power plants or telecommunication networks are aware of the threat from state-backed cyberattacks. When war breaks out, however, any organization or company can find itself being targeted. The NotPetya attack was based on the supply chain of a specialized software package used for taxes in Ukraine, which meant that the victims were only related to the conflict by the fact that they were operating in Ukraine. The WannaCry attack, also in 2017, was conducted for financial gain but has been attributed to state-backed North Korean actors [8]. While these latter attacks caused exceptionally large amounts of economic damage, the cyberattack with the greatest impact on how cyberattacks are understood was Operation Olympic Games of 2010, commonly referred to as Stuxnet [9]. This operation bridged the cyber-physical interface to destroy uranium enrichment equipment in Natanz, Iran. In doing so, it seemed to realize the hopes and fears of many theorists with regards to the potential of cyber warfare, showing that enemy capabilities could be attacked and perhaps even neutralized from any distance, without a shot being fired or a bomb being dropped. Stuxnet generated considerable research interest and showed that cyberattacks can be understood using a broad array of research paradigms and frameworks. It can be understood through technical and forensic analysis of the vulnerabilities and means of attack, in terms of their impact on military strategy, in terms of regulation and legality both on and off battlefield conditions, in exploration of how to conduct them ethically, in terms of strategic deterrence, and so on [10].

While not all this research has been conclusive, the Stuxnet attack accelerated the conception of the Tallinn Manual [11], [12], which provides a practical interpretation of extant law as it applies to offensive cyber operations. It is based on the idea that “cyber warfare is warfare,” i.e. regulated under the “use of force” provisions of the Geneva Convention. Cyberattacks that do not reach this threshold are treated as criminal acts regulated by civilian law. This legal distinction is ir-

relevant to the attackers, opaque to civilian targets who would like improved ways of protecting themselves, and a complication to policy makers who would like to ensure that cyberattacks conducted under the auspices of state power have a net positive cost-benefit ratio. As illustrated by the previously given examples of attacks, there is no doubt that cyberattacks have a far-reaching impact, risk considerable collateral and knock-on effects, and sometimes use these effects for cover. Unfortunately, the calculus involved in their planning and execution is opaque and inconsistent [13]. This thesis aims to investigate the collateral consequences of offensive cyber operations, both in terms of finding workable methods to quantify them, to propose methods to reduce their impact, and through contrasting the costs and benefits of cyberattacks.

The remainder of the introductory summary is structured as follows: Section 2 describes the research background and related work for this thesis. Section 3 outlines the research questions and objectives, followed by an overview of the research methods in Section 4. Section 5 describes the research contributions. Section 6 gives a summary of the appended papers. Finally, section 7 concludes the introductory summary by discussing future work.

2 Background and related work

This section presents terminology and background information to give context for the research presented in this thesis. It provides an overview of the state of cybersecurity research and introduces the concept of Cyber Collateral Damage. This section also describes the research gaps addressed by this thesis.

2.1 Terminology and concepts of cyber operations

As computer security has evolved, and as cyber warfare has become disentangled from information warfare, specialized terminology has evolved. Stabilization of this terminology is recent and to some extent still ongoing. A 2015 survey showed that among 28 countries, standards organizations and reference works, no two had the same definition of “cyberspace” [14]. The Tallinn Manual defines cyberspace as “The environment formed by physical and non-physical components,

characterized by the use of computers and electro-magnetic spectrum, to store, modify and exchange data using computer networks" [11]. This virtual environment has also been designated as a warfighting domain by NATO, alongside the domains of sea, land, air, and space [15].

The terms of art of the cyber domain reflect increasing certainty about what has happened and its intent. A cyber *event* is any discrete occurrence that can be observed and documented. Typical examples include system logins, email received, network packets sent. For an event to be considered an *incident*, it must be an "anomalous or unexpected event, set of events, condition, or situation" which "actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits" [1], [16]. Thus, while a cyber incident does not need to be harmful, it must at minimum risk harm to organizational security or data. When cyber incidents are caused intentionally, they are called *cyberattacks*. Many cyberattacks take the form of *denial-of-service attacks*, which are cheap and easy to execute. These attacks attempt to consume and exhaust some limited system resource, i.e. network bandwidth, server memory, mailbox size limits, etc.

One of the primary purposes of information systems and computer networks is the safe storage and transmission of sensitive data. When such data is exposed in a cyber incident, the incident becomes a cyber *breach*. Legislative and technological safeguards exist to prevent and reduce the harm from cyber breaches, including encryption, access controls, and other privacy-enhancing techniques.

Cyberattacks launched by nation-state actors, and especially by military actors, are sometimes referred to as *offensive cyber operations* or OCOs [17], [18]. In terms of quantity, these form a minority of cyberattacks and breaches, with the great majority being conducted by private citizens for criminal financial gain [6]. Many of these attacks are controlled by organized gangs in key regions where national governance is lax [19]. These gangs form a cyberattack ecosystem, which is not only tolerated but actively used by states as a force multiplier, blurring the lines between crime and espionage. Notably, criminal gangs have been used to conduct cyberattacks in the Ukrainian conflict [20]. Nevertheless, Offensive Cyber Operations can be considered the building blocks of *cyber warfare*. "The term 'cyber war-

fare' [...] is not necessarily used to denote scale or protraction, or even 'violence' per se, in the sense of a 'war' as it is perhaps generally understood. [...] [It] is used to denote 'warlike' acts, [it] is employed broadly to convey an interstate element in the use of technological force in cyberspace" [21]. This distinction separates cyber warfare, generally accepted as describing conducted cyber operations in aggregate, from *cyber war*. A cyber war would be a war conducted solely or primarily in the cyber domain, perhaps through the use of devastating vulnerabilities in the stockpile. The exact threshold to cyber war is uncertain, but while there are strong arguments made that it has not arrived and perhaps will not ever arrive [22], [23], there are few recent counterarguments.

The "CIA" framework frequently used in computer security describes the essential information system properties targeted by cyberattacks; those of *confidentiality*, *integrity*, and *availability* [24], see Figure 2. Cyberattacks will target at least one of these three properties to exfiltrate or alter data, or to prevent it from being accessed. Confidentiality attacks include hacking and data breaches, where the attacker will attempt to steal sensitive data to use or disclose it. Integrity attacks include man-in-the-middle or tampering where information is planted or altered, or where malicious code is injected for future effect. Availability attacks are exemplified by (Distributed) *Denial of Service* (DDoS/DoS), where systems are flooded and overwhelmed by requests, taking them offline or making them inaccessible.

Figure 2. The Confidentiality-Integrity-Availability triad.

2.2 The myth and promise of cyber warfare

Military commanders have always dreamed of action at a distance. Ideally, this action should also be unattributable to its source, or plausibly deniable [25]. Cyber operations seemed to provide both a new avenue of attack and a new threat to deter and defend against in a world with fewer shooting wars and increasing amounts of cold wars, trade wars, and small conflicts [26]. A central question in the initial understanding and theorizing of cyber warfare thus concerned its potential for a bloodless but highly destructive attack, perhaps a decapitating strike, across the cyber domain [27]. This attack could potentially knock out power plants and other critical infrastructure, as well as national news media, leaving an opponent cold and confused with the press of a button.

The technical realization of cyberattacks typically involves the identification of previously unknown vulnerabilities in software, known as zero-day vulnerabilities [28]. While it is in the public interest to disclose and close such vulnerabilities when they are discovered, an actor planning and preparing to exploit them in an attack can collect and stockpile such vulnerabilities to retain the potential to use them at a

later date. Leaks from various intelligence agencies have shown that this practice of collection and preparation is widespread, and the destruction caused by these leaks have also given credence to the potential in such attacks [29]. In addition, advanced threat actors will go beyond naturally occurring vulnerabilities and will instead develop and insert backdoors and malicious code into commercial and open source software for their own use. While these vulnerabilities typically depend on programming flaws leading to buffer overflows, code injection, or other technical means of attack, they can be understood at high level through the PReP framework [30]. This framework classifies vulnerabilities by

1. Propagation method,
2. Exploit, and
3. Payload.

Although the payload is typically developed or customized for attacks against a specific target, the exploit can be more generally applicable and is, in fact, more valuable the broader its use. Exploits can also be bought and sold, commanding high prices on illicit marketplaces. With the rise of the Internet, Propagation is often across computer networks. As a line of defense, many sensitive networks are air-gapped, i.e. physically disconnected from Internet access. These systems must be attacked in a combined operation, perhaps by finding an operative who can smuggle a USB stick across the gap.

In the earliest cyber operations, such as the Russian "Moonlight Maze" attack on US defense systems in 1996, the *payload* was systems access used to steal sensitive data [31]. Thus, cyber warfare was closely intermingled with information warfare for the first decade of its existence. In 2007, large-scale Denial of Service (DoS) attacks against Estonia caused an increase in research and defense interest, especially as these were partially crowdsourced to non-state actors to increase their destructive power [32], see Figure 1.

Figure 1. Screenshot of attack instructions spread to non-state actors in 2007, captured by [32].

While the 2007 Estonian attacks piqued public interest, they could still be understood in terms of information warfare, and their impact was ultimately limited. It was the 2010 Stuxnet operation which changed the playing field by exhibiting three characteristics. First, it was highly publicized. A cyber operation against a secret nuclear weapons program was attractive to news outlets around the world. Second, the operation was successful. The exact level of success is disputed and will perhaps never be fully known, but the Iranians were certainly humiliated and as many as one fifth of centrifuges were destroyed. Third, the operation spread widely outside of the target area, causing considerable collateral damage. Later analysis showed that safeguards had been put in place specifically to reduce unintended harm, evidence that collateral damage was on the minds of the designers.

With evidence of a successful cyberattack against a critical cyber-physical system, US Defense secretary Leon Panetta warned that an aggressor nation could execute a “cyber Pearl Harbor” where they would “derail trains, contaminate the water supply, or shut down the

power grid" [33]. This defense sector narrative of a world at the mercy of decapitating cyberattacks was discussed and examined without conclusive evidence as no such attack materialized, even when Russian forces invaded eastern Ukraine in 2014 [22], [34]. The continuation of the Russo-Ukrainian war has caused critical re-examination of the role and value of cyber operations in warfare. Meanwhile, there are now 34 countries in the world known to actively use cyber capabilities to conduct open or clandestine operations [35]. Until a "cyber Pearl Harbor" materializes, cyber capabilities must continue to be conceptualized and understood in terms of defense economics and national security, while acknowledging their role in warfare—even when that role is less impactful than some would wish or fear.

2.3 Offensive cyber operations as a research topic

The earliest research publications considering the potential of "cyber war" concerned information systems being used to wage information-based warfare [36]. Computers and networks were seen as bearers of information that could be stolen or manipulated. While this early thinking was prophetic, it was restricted to considering value in terms of information gathering and damage in terms of confusing the enemy. Nevertheless, the use of computer networks as a domain of attack and defense began to be explored from technical, political, ethical, and legal angles [37], [38]. This development also brought the term "cyber" to denote attacks across computer networks, and the general idea of "cyberattack" as a significant danger to society [39].

Technical research on cyberattacks is predominantly seen through the lens of conventional cyber security research, focused on preventing attacks and primarily reducing the harm from cybercrime. This harm reduction is realized by making systems more inherently secure through secure programming practices and system setup, by educating users on security awareness, by unmasking and crippling organized cybercrime gangs, and so on. Defending an environment against offensive cyber operations has considerable overlap with securing it against cybercrime. When it comes to the legal angle, however, the differences multiply. State-backed cyberattacks bring an additional challenge in tying the attack to a specific threat actor, as attribution is required for international law to apply. There are significant political consequences of attribution even with ironclad evidence [40]. These

consequences, taken together with the inherent complexity of finding sufficient proof, mean that public attribution is a policy question more than a question of forensics or technical analysis [41].

Attacks which are attributed can be checked against the "use of force" provision, e.g. by utilizing so-called "Schmitt Analysis" against a list of seven criteria derived from Article 2(4) of the United Nations Charter [38]. Attacks meeting the criteria are considered equivalent to armed attack and may face lawful retaliation. They also fall under those Laws of Armed Combat that apply to the protection of civilians and civil infrastructure. Although the threshold is rarely acknowledged to be crossed [42], and has never by itself been used as *causa belli*, it is enshrined in cyber doctrine. The 2023 United States Cyber Strategy calls for "[the use of] cyberspace operations for the purpose of campaigning, undertaking actions to limit, frustrate, or disrupt adversaries' activities *below the level of armed conflict* and to achieve favorable security conditions" (emphasis added).

Thus, the study of cyberattacks has been informed by extant legal frameworks even when the actors involved do their best to avoid the restrictions imposed by those frameworks. An alternative angle of examination is that of cyber ethics, which ask the questions of why and if offensive cyber operations are just and proper for states to undertake [43]. While the justified reasons for war and the ethical conduct of war have been studied for millennia, the interconnected nature of cyberspace and the ease with which plausibly deniable attacks can be conducted mean that norms and rules need to be re-examined.

These examinations inevitably intersect with questions of state policy and military doctrine. While technical analysis provides a blueprint for actions needed to secure systems, the means and budget afforded to cyber defense are analyzed through security studies. Conferences on the hot-topic issues of cyber resilience and cyber sovereignty—technical independence from services produced in other countries—cater equally to cryptographers and foreign policy specialists. All in all, the field is broad and often interdisciplinary. One of the few unifying factors is the dominance of qualitative analysis. Data is scarce, and disentangling state-backed operations from the masses of cybercrime is time-consuming [44].

Even where data can be found, there are few agreed-upon metrics of comparison. The concept of military utility as proposed by Andersson

et al. [45] has not yet gained widespread acceptance, with military planners preferring to measure mission success against predetermined sets of criteria. Strategic-level metrics such as human lives lost or GDP impact have historical weight as well as broad and intuitive acceptance but are less appropriate to pure cyber operations. Qualitative understanding of the impact of cyber operations is still in its infancy.

2.4 Civilian harm and collateral damage

In the latter half of the 20th century, an international consensus grew around the desire to limit the horrific impact of war upon civilian populations. One tangible outcome of this effort was the 1977 Additional Protocol to the Geneva Convention, which seeks to protect civilians and civilian objects. The protocol harmonizes with the desire of nations considering themselves as virtuous to implement legislation defining what had previously been considered only as norm. Within the cyber domain, there are numerous credible reports that military cyberattacks have been stopped due to the expectation of collateral damage. As early as 1999, the Pentagon reportedly considered hacking into Serbian computers but held off after receiving guidelines warning them that civilian harm from cyberattacks could subject US warfighters to war crimes charges [46]. It is possible that they stayed their hand for fear of escalating the acceptable level of cyber-war in coming years, or for fear of appearing less virtuous, rather than because of any legal ramifications under international laws or treaties. Moreover, these considerations can be kept precise and specific only because collateral damage has an exact definition in terms of military operations, but offensive cyber operations are sometimes conducted by non-military state actors who do not fall under the Law of Armed Conflict, or in conditions that do not fulfill the legal threshold for attacks or acts of force [47]. Indeed, Rid [22] argued that no military cyber operation had ever reached the threshold of an armed attack (as specified in the UN Charter or NATO article 5), although the Stuxnet operation was generally accepted to have been an “Act of force” [48]. Two factors considerably complicate this model. The concept of collateral damage contains an underlying assumption of virtuous intent, where attacks are not intentionally causing civilian harm. In addition, below-threshold attacks are legally equivalent to espionage, which is

not regulated in international law. Responding to these below-threshold attacks can be done in one or more of at least five separate ways, listed in table 1.

Table 1 Response domains for below-threshold cyberattacks.

Domain	Response
Diplomatic	Sanctions against countries, organizations, and people, including banking-based measures.
Criminal law	National justice system and international organizations like INTERPOL and UNODC.
International law	Applying the laws of armed conflict.
Technical measures	E.g. blocking internet providers, IP address ranges and domain names.
Military force	Counterattack and deterrence, typically though the cyber domain.

Of these responses, the most well-researched is that of international law. It is also the only response which has not seen practical use, although the ICC has indicated that they are ready to try cases from the Ukraine war [49]. The relationship between the threshold of force and the intentionality of the attack is illustrated in Figure 3.

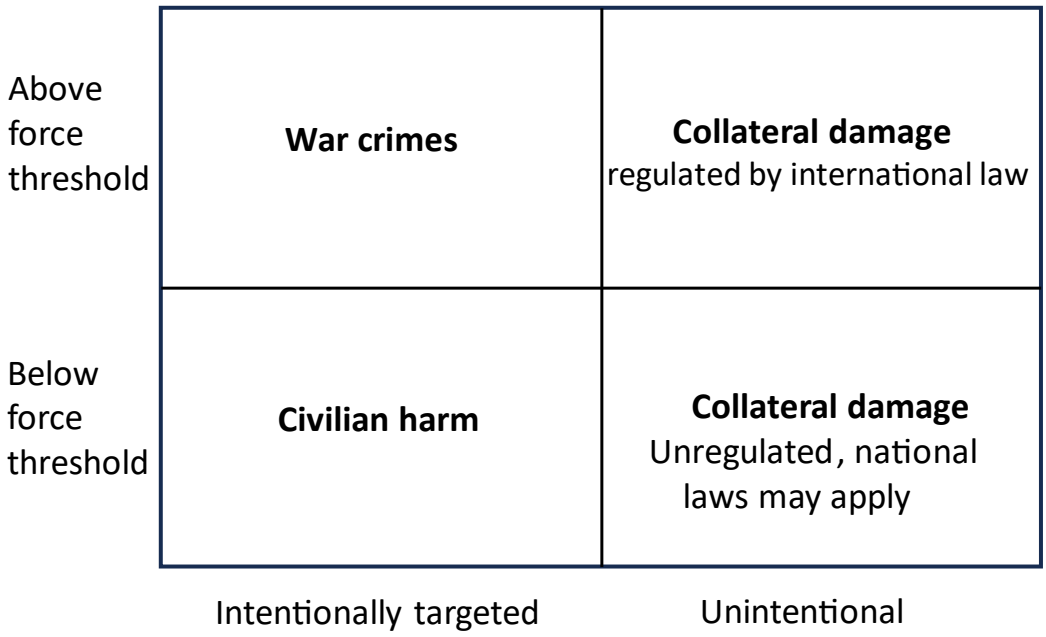

Figure 3. Types of civilian impact from cyberattacks.

This understanding of collateral damage is based on law and of ethics, and its public perception is often understood primarily in terms of physical harm and loss of life. Analysis of cyber warfare is sometimes based in the Clausewitzian understanding of war as the unfettered continuation of politics by other means [50]. While that can certainly hold true when cyber operations are part of an industrial and attritional conflict like the Russo-Ukrainian war, the destruction of civilian property, while less objectionable to the public, is now equally protected by law. Only when these laws are disregarded and remain unenforced is attritional cyber conflict possible.

The application of economics to war was one of the first uses to which that science was put. Throughout the 19th century and well into the 20th, this application was also generally Clausewitzian, concerned solely with maximizing the production of war materiel. It took until the 1970s for research questions to shift towards accounting for the total cost of conflicts [51]. Such an accounting considers the value of physical, natural, human, and social resources destroyed, as well as opportunity costs of lost output and increased allocative inefficiency [52]. Within the field of economics, an externality is an indirect cost to an uninvolved third party caused by another party's activity. Utiliz-

ing the concept of externalities when conducting econometric analysis of complex and interconnected situations means that costs and benefits to society can be identified, quantified, and compared directly, in monetary terms. Warfighting has historically been rife with externalization. A retreating army will blow up a bridge to stop a pursuing enemy without hesitating even for a moment to analyze the cost of rebuilding it. When there is a risk to noncombatants, the law of armed conflict has necessarily led to an increasingly systematic approach to reduce that risk. Traditional Collateral Damage Estimation (CDE) methodologies are based around models more commonly found in risk management [53], as shown in Figure 4. These models typically use coarse-grained levels of potential damage to structures and civilians in order to answer what restrictions are necessary in weapons management, as well as to help determine whether to authorize an attack at all. The challenges in quantifying the value of lives lost also mean that structural damage is the main parameter considered when determining the economic value of collateral damage.

Risk to mission →

CDE Level	1	2	3	4	5
Structural Damage	No	No	No	No	Yes
Casualties	No	No	No	No	Yes
Restrictions	None	Weapon	Weapon, Fuze	Weapon, Fuze, Delivery, Heading	

Figure 4. Collateral Damage Estimation Model, based on [53].

Borrowing from the understanding of natural disasters, civilian harm can lend itself to econometric quantification. Rowe [54] used actuarial values (e.g. $50 000 per year of life lost) as a starting point for back-of-the-envelope calculations of the cost of cyber operations. This approach is crude, but useful, as the number of lives lost as a direct result of such operations is likely to be small [22]. In addition, the cause-and-effect chain of cyber operations is considerably more opaque than in earthquakes, weather events, or conventional warfare. Moreover, the analogy between collateral damage from conventional, kinetic warfare and cyber-warfare holds true when cyber operations spread and spill into non-targeted systems. This is both a conse-

quence of cyber weapons being designed to spread across networks in order to reach across firewalls and air gaps, and because each cyber-weapon consists of executable computer code which can, with the requisite effort, be reused by anyone in a position to intercept the attack. This is wholly unlike kinetic munitions, which do not drop from the sky with drawings and materials attached. In summary, while the understanding of cyber collateral damage has developed from origins in conventional warfare and the cost estimation of natural disasters, laws, norms, and estimation models have not yet been fully adapted to the cyber domain. These issues are investigated further in Paper III and Paper V.

3. Research questions and objectives

Collateral damage from cyber operations is more than just an academic concern—it presents real-world challenges for policymakers, military planners, and civil society. By their nature, cyberattacks are unpredictable in scope and effect. While conventional military operations usually have well defined battle zones, the boundaries of cyberspace can be porous. The interconnected nature of cyberspace means that malicious cyber activities targeted at a particular entity or system can more readily spread or escalate beyond what is desired.
The main goal of this thesis is to improve the understanding of the benefits and costs of offensive cyber operations, especially when those costs are unintentional in nature, as well as to propose methods for quantifying and reducing said costs.
The following research questions (RQs) are considered:

RQ 1: *What problems, gaps, and challenges exist when considering collateral damage from offensive cyber operations as a research topic?*

The thesis considers this question both in terms of what collateral damage means in the cyber domain, how it has been investigated in research, and what gaps and challenges remain. Through a review of prior research, a research domain can be identified and categorized. This review will be able to survey and collect gaps and problems identified previously but left unaddressed.

RQ 2: *How can the collateral damage and proportionality of Offensive Cyber Operations (OCOs) be quantified?*

RQ 3: *How can the collateral damage of OCOs be reduced or mitigated?*

These interrelated questions require methods of collateral damage estimation (CDE) adapted to cyberspace. The research on CDE for cyberspace operations is still in a fledgling state, with Pascucci [13] observing that "there is no established collateral effect (damage) estimation methodology, causing all assessments to be subjective and largely inconsistent." Ideally, this thesis will advance the development of an openly available CDE model for cyberspace operations. A particular area of interest is externalized costs, which are ignored or accounted for in planning or effect estimation.

4. Research methods

This section describes the applications of research methods in the thesis, as well as providing a rationale for their selection. Choosing the appropriate research method is not only a function of the research question itself, but in a situation where multiple appropriate methods are available, the choice will inform the way in which the question is answered. As noted in the background section and further investigated in Paper I, most research considering collateral damage from cyber operations is qualitative in nature. Some of these studies utilize a first-principles approach, whereas legal works use so-called "black letter analysis," focusing on interpreting the letter of the law. This thesis utilizes mixed methods research to answer the research questions, combining qualitative and quantitative methods, and uses a two-phase approach. The first phase is focused on answering research question 1 and is conducted with a structured literature review. The second phase is intended to answer research questions 2 and 3 by using case studies and quantitative analysis. The relationship between the phases, the research questions, and the appended publications is illustrated in Figure 5. The publications have been ordered according to their place in this structure, rather than by date of publication.

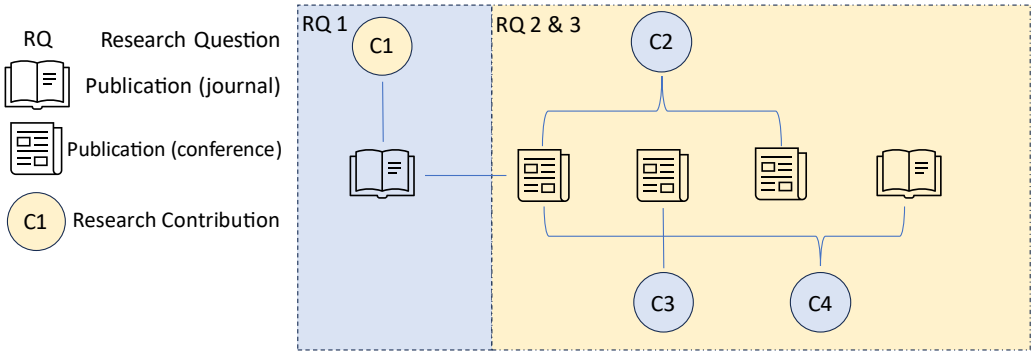

Figure 5. Research questions, publications, and contributions.

4.1 Epistemological approach

While computer science is a modern field, its philosophical underpinnings and investigative methods have grown out of the field of engineering sciences, mathematics, physics, and of natural sciences in general [55]. As such, it typically utilizes empirical observations and real-world experiments to understand and mathematically model the behavior of systems. While this thesis partly utilizes qualitative methods that are sometimes associated with interpretation challenges common to social science, such as case studies, the cases are constructed using observed events rather than (e.g.) interviews. In addition, the role of the researcher in understanding the data is taken to be detached and neutral, with the studies being constructed to be independently replicable. To further this cause, all data gathered in the research for this thesis are openly and wholly made available for further study (e.g. [56]).

4.2 Mixed methods research

When considering cyber warfare research, quantitative methods can be used to determine the technical attributes of attacks—frequency, duration, exploit, payload used, and so on. Determining the cost or the utility of the attack requires the use of qualitative analysis, including the valuation of intangibles, policy assessment, or determining political goals. These qualitative data can then be used for hypothesis building or quantified to develop or test mathematical models. The combination can have an impact on design complexity and requires the researcher to develop the necessary mastery in each separate method used. The additional time and cost required must be weighed against the increased understanding gained.

Although mixed methods research can utilize different designs, sequential approaches are easiest to adopt since they "facilitate the integration process of [...] studies [...] at the cost of higher implementation time" [57]. The research covered in this thesis followed a more complex two-phased design. In the first phase, research was centered around a large dataset of security protocol adoption across the Internet and the questions which could be answered using that data only, leading to Papers II-IV. In the second phase, insights from the first phase were integrated into a broader and deeper outlook of the field with additional data sources in Paper V, with the literature utilized throughout the research being compiled into a standalone review (i.e. Paper I).

4.3 Systematic Literature Review

Research on cyberattacks and cyber warfare goes back only to the late 1990s but has evolved rapidly. Sufficient literature now exists for the field to be amenable to systematic review, e.g. as described by [58]. Such a Systematic Literature Review (SLR) can capture gaps in the literature and thus identify areas where further research is needed. A significant portion of this research is technical and qualitative, but not narrative, which means that it is amenable to categorization and thematic analysis [59]. In addition, the SLR can identify relevant theories and frameworks to utilize, ensuring that the research encompassed in the thesis is grounded in and aligned with the field. Thus, an SLR on collateral damage from cyber operation was conducted in Paper I. The review was systematic but not exhaustive; it utilized five scientific databases (IEEE Xplore, ProQuest, ScienceDirect, Scopus, and Springer Link) chosen for their coverage and assessed probability of containing relevant publications. The search methodology and assessment for inclusion or exclusion was conducted according to the University of York Database of Abstracts of Reviews of Effects (DARE) Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) criteria [60]. The included papers were qualitatively assessed to identify recurring themes and trends in the research area, as well as for potential gaps in need of further research.

4.4 Case study

Cyberattacks are based on technical properties and vulnerabilities of systems, but also utilize social dynamics and psychological weaknesses in their execution. The effects of these attacks are realized in technical, economic, and societal contexts. A case study can draw on multiple data sources to allow for a richer understanding of how these various contexts interact [61]. The goal is to not merely describe a sequence of events but to find insights or theories with broader applicability. Previous case studies in cyber security and warfare contexts have looked both at one specific attack [62] and compared multiple attacks [63].

Case studies also provide a real-world context for models and simulations. As such they can be used to validate or refine them by comparing their predictions or results against observed outcomes. If the model does not hold, a case study can reveal uncaptured or underestimated variables which impact outcomes, such as system interdependencies or sociopolitical factors. Paper II used a case study of a cyber incident with high collateral effects to develop a time-to-target model. Although this incident was based on a vulnerability which could not be attributed to intentional implantation by a state actor, irregularities in the disclosure of the incident made it clear that the vulnerability was known to some party or parties. The model assumes that the vulnerability is implanted for use as a back door and predicts the time until a given percentage of systems have updated to the vulnerable software version. Longer propagation times risk increasing the collateral damage caused, as systems will be open to attack for longer. To evaluate the predictions of this model, a longitudinal study was conducted in Paper IV. In an additional case study, Paper IV attempted to generalize the model using new datasets from other similar software packages. Finally, the findings of the case study in Paper II were used as the basis for theoretical model improvement in Paper III.

4.5 Quantitative analysis

Utilizing a quantitative, data-driven approach means data must be made available, which can be a challenge in a field characterized by secrecy. Both the attacker and the attacked can have a vested interest

in keeping the details of cyberattacks to themselves. Datasets of cyberattacks are frequently based on news articles or secondhand sources (e.g [64]). First-hand information is either leaked and unverifiable, or declassified after enough time has passed. Extracting truths from this biased data is a considerable challenge. Nevertheless, quantitative research can be less sensitive to researcher bias and more replicable than qualitative research, especially in immature fields or where the terminology is unstable. In addition, very few quantitative studies have been performed on cyber warfare. In the greater field of cyber security, quantitative modeling and analysis is more common, e.g. when measuring the defensive costs of corporations and cyber-insurance payouts [65]. Through a combination of existing cost estimates from general cyber incidents and cyberattack data from the Ukrainian conflict starting in 2014, Paper V applied quantitative analysis to find the total cost of cyber warfare. The methods used were cornerstones of research economics, bottom-up accounting and counterfactual analysis. Although data availability and the practicability of the method was not guaranteed in either inquiry, a positive result in one and a null result in the other would still provide valuable for future research.

4.6 Ethics in research and in the open study of cyber warfare

The ethical conduct of research requires a balance between different competing interests [66]. To help strike this balance, the European Federation of Academies of Sciences and Humanities provides four fundamental principles for good research practice [67], listed in Table 2.

Table 2 Fundamental principles for good research.

Principle	Description
Reliability	Good research quality through careful choices in research design, methods, and analysis.
Honesty	Transparent development, conduct, and reporting of research.

Respect	Due regard for the rights and time of research participants, colleagues, and society as a whole.
Accountability	End to end responsibility of knowledge development, publication, and use.

Although every work of science will encounter issues related to each principle, the issue of *respect* is critical to this thesis where it uses datasets containing personal information. The interest of bettering society through research must be balanced against the privacy rights of the individuals. Complex issues arise when said individuals are the targets of a cyberattack. For public figures, e.g. the chancellor of Germany, inclusion in a research database like that collected for Paper V may be permissible. For low-level Ukrainian military officers, it may not be. External datasets must be validated for ethical practices in collection and for appropriate treatment of personal information. The Paper V dataset was anonymized as part of processing and publication.

On the other side of the balance is the net benefit research creates in society. The cyber domain is often opaque by nature, and the various actors found in cyber warfare often use and rely on secrecy. Some cyber operations are classified under the auspices of national security, and the nature of classified operations is such that an external observer cannot determine whether the secrecy of the project is defensible. Nevertheless, open and *honest* research into these operations (i.e. research that uses unclassified sources and methods, and openly publishes results) can be of net benefit to society. Such research has additional responsibilities beyond the four defined by ALLEA—it must not expose sources or methods of secret operations and should not unduly risk increasing the unnecessary harm of warfare.

Cyber operations frequently use undisclosed vulnerabilities to uncover sensitive data, and researchers in the cyber domain sometimes come across one or both, i.e. as in Paper II. The field's gold standard for this situation is known as "responsible disclosure," based on the idea that the organization responsible for addressing the vulnerability will get a reasonable chance to do so before it is made public. Here, at least three different legitimate interests are in conflict:

- The agency which has discovered (or sometimes, implanted) the vulnerability and wishes to use it operationally,
- The organization or company which would like to protect its reputation and the security of its stakeholders and customers, and
- The general public, which deserves to know about risks it might face in using a certain piece of software or interacting with a certain organization.

These interests must be balanced, but the balance of power is normally in favor of well-funded companies and government agencies. Through *accountable* but rapid disclosure of vulnerabilities, science can be put in direct service to the public.

Finally, extending econometric models into cyber operations can improve (or disprove) the generality of those methods [68]. An example is the use of contrafactual analysis to compare economic development in a country affected by offensive cyber operations to a panel of similar countries which were not affected, as in Paper V. While this method is generally accepted as valid in the economic domain, *reliably* extending it into a new domain by application will continue to shed light on its usefulness and broad applicability. This benefits both the "originating" field of economics, further strengthened in the new knowledge that its methods are universal, and the "receiving" field of cybersecurity, which will be able to draw on existing research. A mature field of research will have a commonly agreed body of knowledge and set of research methodologies. A developing field, like cyber security, will either invent new and novel methods, adopt existing methods from other fields, or reinvent the wheel by unknowingly reinventing existing methods. These later, reinvented methods represent wasted resources and a risk of confusion both in terminology and reusability of the domain-specific techniques.

4.6 Limitations

The studies contained in this thesis each have limitations which contribute to limitations of the work as a whole. These stem from considerations and potential biases in data collection and analysis, as well as from problem selection and formulation. One such limitation lies in the evolving terminology and nomenclature of cyber security research. For instance, the preferred term of art for a given operation

may have been “information warfare” in the 1980s, “computer network attack” in the 1990s, and “cyber warfare” in the 2000s. Nonstandard terminology may lead to gaps in understanding of the research field or wasteful reproduction of previous work. Although the terminology around “cyber” operations has gained acceptance, there are still dozens if not hundreds of contending definitions for each term [14].

In addition to potentially missing papers with nonstandard terminology, the literature review on cyber operations and collateral effects in Paper I used a limited set of scientific databases. The search methodology was also based on titles, abstracts, and keywords rather than a full-text search with many more false positive matches. It is a virtual certainty that further papers of interest exist but are not indexed in these specific databases or in the fields searched. This risk was mitigated through the use of snowballing techniques, but there is always the potential to find more material with a deeper and more exhaustive search. The papers found in the review were assessed for content by only one reviewer, the author. There is thus a risk of bias in source selection causing skewed results. This bias could have been mitigated by having multiple people independently assess suitability according to the inclusion criteria. Having a single reviewer improves consistency in selection but also increases the risk of bias. A final risk of bias to consider is based on the publication process itself. Papers available for study are likely to be skewed towards publishable results, rather than null or negative results [69].

Beyond scientific search engines and open research, there is a wealth of confusing and contradictory data on cyber operations to be found in news media and press releases. This data is typically made available either by the defender or by third-party investigators and may be heavily biased or intentionally misleading. In addition, the attacker’s perspective is virtually certain to be missing, or at best drawn from exercises and simulations. This thesis takes the same approach by necessity, drawing on higher-quality sources for defensive approaches and bottom-up costs of victims, but simulating and guessing at attacker motivations in Paper II and Paper IV. Although the bottom-up cost analysis in Paper V was done with all due care, data availability precluded counterfactual analysis of the reference scenario. This means that the cost estimate found by bottom-up accounting could

not be verified. In addition, a sensitivity analysis has not been performed. Consequently, the validity and the precision of the estimate is uncertain.

5. Contributions

In attempting to answer the research questions posed in this thesis, the following contributions have been made (see Figure 5):

1. *A systematic understanding of the literature on Cyber Collateral Damage*
   This thesis reviewed and systematized existing research on collateral damage from offensive cyber operations. This review reveals categories and clusters of research which generally have limited overlap. In particular, the main source of understanding of cyber collateral damage is through legal scholarship of black-letter international law. A considerable gap exists between this perspective and the practical circumstances of below-threshold operations.
   The research further identified a gap in targeting techniques. Military operations often use the Joint Targeting Cycle [70] to methodically analyze, prioritize, and assign targets. While this process has been proposed for cyber targeting, there is no research consensus or common doctrine. Improved targeting would strongly contribute to reduced collateral damage from cyber operations.
   The results of the review directly address RQ1.
2. *A model for and longitudinal study of the benefit when conducting offensive cyber operations against hardened targets using techniques with a high risk of collateral damage.*
   Using an open dataset encompassing hundreds of thousands of Internet-connected servers, the research modeled the uptake of a vulnerable security library. Hypothesizing that this vulnerability was intentionally implanted, the research included the creation of a model which considers the potential utility gained in terms of time to reach the target. Using this model, an initial time-to-target estimate was made; two years for 50% coverage and four years for 75% coverage. Revisiting this prediction seven years later, a follow-up study validated the prediction. The

research also attempted to generalize the model to other security protocols but determined that it could not be directly applied. This assessment of cyber implantation utility contributes to answering the second part of RQ2.

3. *A proposed extension to a research model of the web security ecosystem*

   Investigating a model of the Secure HTTP ecosystem by [71], the thesis proposes an extension which adds regulators and standards organizations as actors in the model. This extension is intended to improve the utility of the model by making it possible to consider additional interactions and relationships. In particular, these actors will have a central role in reducing the ability of other actors to externalize security costs, and in setting and spreading best practices to other actors. The application of best practices will improve industrial cyber security and reduce collateral damage, addressing RQ3.

4. *An assessment of the applicability of different econometric methods to cost estimation of cyber operations, with a sample bottom-up estimation in the context of a specific cyber conflict.*

   Beginning from the econometric study of conventional warfare, the research adapted bottom-up cost accounting to the cyber domain. Doing so makes it possible to draw direct parallels to the estimation of cyber incident costs. To show the practicability of the method, the researchers collected and separately published a data set of cyber operations in Ukraine 2013-2021. Using this dataset together with cost estimates from industry and insurance estimates, it was possible to give a societal cost estimate for the conflict. Doing so addresses the first part of RQ2.

   The research also investigates the methods used to reduce both direct and collateral damage in the first part of the Ukraine conflict, noting that the most efficient such method was the migration of government information systems to cloud service providers in NATO countries. While many nations are still mainly concerned with sovereignty in service production, protected cloud services could help reduce collateral damage, addressing the second part of RQ3.

Finally, the research assesses the applicability of counterfactual cost analysis to the cyber domain but concluded that sufficient data is not yet available. In gathering data, the researchers called for more standardized taxonomy and common measures of granularity in incident recording.

6. Summary of Appended Papers

Paper I - Collateral Damage from Offensive Cyber Operations – a Systematic Literature Review

This paper investigated research on collateral damage from offensive cyber operations, or cyber collateral damage (CCD), by conducting a systematic literature review. Five different scientific databases (IEEE Xplore, ProQuest, ScienceDirect, Scopus, and Springer Link) were searched for relevant publications. The review revealed that the field of CCD research clusters into legal, targeting, ethical, taxonomic, econometric, and estimation & modeling research. The paper identified research gaps and trends, especially related to the lack of interdisciplinary collaboration across research areas. It also made policy suggestions for national cyber doctrines and the future of the Tallinn 3.0 process.

Paper II - Determining the Utility of Cyber Vulnerability Implantation - The Heartbleed Bug as a Cyber Operation

By implanting a vulnerability in software known to be used by a hardened target, an attacker can create opportunities for a future breach — a supply-chain attack. This paper explores a case study constructed by considering a recent and highly publicized zero-day vulnerability in the open-source OpenSSL library, and by hypothesizing that the vulnerability was introduced intentionally by a threat actor. Using a large dataset collected from hundreds of thousands of Internet-facing systems, a model for adoption of security software over time was created. Using this model, the paper predicted 50% coverage of targets in two years and 75% in four years and suggested that these time frames could be used for cost-benefit analysis. In addition, the model was constructed to be adaptable to other circumstances of security protocol or feature adoption on the Internet. The paper concludes that while implanting zero-day vulnerabilities can be a workable method

of attack, such operations take time and incur non-negligible risks of collateral damage and other societal costs.

Paper III - Papering over the cracks: The effects of introducing best practices on the web security ecosystem

This paper considers a model of the web security ecosystem introduced by Arnbak, Asghari, van Eeten, and van Eijk [71]. The main contribution of the paper is an extension of this model by adding standards organizations and regulators to it. The roles of these actors are defined and described. The goal in extending the model is to find ways of improving resilience against supply chain attacks like those considered in Paper II. In addition, the paper extends the time series of Paper I, but these extensions are wholly covered by Paper III and described further in that context.

Paper IV - Cyber Vulnerability Implantation Revisited

This paper revisited the predictions made in Paper I by extending the study longitudinally over seven subsequent years. The contribution of the paper was to validate the predictions, and thus to ascertain not only that the model was correct but also that the methodology of model construction was practicable. In the longitudinal follow-up, the short-term predictions (up to four years) were validated with low RMS error, but the asymptotic adoption behavior was not. The paper also checked the model against the rollout of the next web security protocol, TLS 1.3, observing that it was not generalizable due to changing conditions of web service providers.
Finally, the paper analyzed the decline of insecure and vulnerable protocols, noting that these tend to remain essentially forever on a small fraction of systems.

Paper V - Towards econometric estimation of the societal cost of cyber conflict

This paper investigated how a full accounting could be made of the costs of cyber conflict by considering two tools from econometrics, counterfactual analysis and bottom-up accounting. The paper describes the application of each of these models to the domain of offensive cyber operations, noting that counterfactual analysis is hampered by data availability and the size of the effect being studied compared

to commonly available figures, e.g. GDP. Instead, bottom-up accounting is used to conduct a case study estimating the aggregate societal cost of cyber conflict in the Ukrainian war between late 2013 and 2020. A dataset of 76 was assembled and analyzed to show the method in practice. The societal cost of these cyberattacks was estimated to be $160M.

7. Conclusions and future work

There is a multitude of different theoretical frameworks which can be applied to cyber operations. However, data availability, attribution issues, and national security considerations have so far made it unusual to find open research applying quantitative analysis analyzing them as events with costs and benefits. This thesis proposes that an under-investigated metric for such analysis is economic cost, and that the societal totality of this economic cost is subject to considerable externalization in the planning of cyber operations. In the context of wartime exigencies, ignoring or deferring external costs may be reasonable. However, most cyber operations are intentionally conducted below the threshold of force. This thesis has shown that such operations can require multi-year dwell times, leading to an increased risk of collateral effects. In addition, it seems exceedingly unlikely that these effects are sufficiently understood, or that they are systematically taken into consideration when planning and executing an attack. To expand the view on offensive cyber operations, this thesis has adapted economic models and data from conventional warfare and industrial cyber security to cyber warfare.
The data scarcity of the field creates challenges in answering to what degree investments into cyber capabilities are worth it. For many years, cyber warfare seemed to promise a bloodless solution to future wars. In practice, the cyber domain is still poorly regulated and consumes vast sums in industry spending on cyber security, as well as unknown but significant parts of defense budgets, disproportionally to the collateral costs incurred.

Although cyber warfare provides action at a distance, the effects have been limited. While this research has estimated the societal cost of successful cyberattacks to be small compared to GDP and to the po-

tential costs of other forms of warfare, the defensive costs cannot be discounted and require further analysis. Conversely, the production costs of state-backed cyber operations could be estimated based on cyberattack pricing in the open market. As most cyber operations are below the "use of force" threshold, such cyberattacks require dedicated study and a response taxonomy. Researchers can help determine which criteria determine the most effective response domain. To this end, it is valuable to study and interface with the ongoing work of producing the Tallinn Manual 3.0 as well as the United Nations Open-Ended Working Group "on security of and in the use of information and communications technologies." In addition, the diplomatic and legal responses in current use can be complemented by technical tools. The efficiency of opt-in network blocking solutions like the Criminal IP C2 and Spamhaus XBL block lists could be evaluated, and if found sufficient could form the bases for national or international solutions to rapidly block threat actors.

References

[1] NIST, "Special Publication NIST SP 800-82r3 Guide to Operational Technology (OT) Security," 2023.

[2] B. Aiyer, J. Caso, P. Russell, and M. Sorel, "Mckinsey: New Survey reveals $2 trillion market opportunity for cybersecurity technology and service providers," https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers.

[3] Verizon, "Verizon Data Breach Investigations Report 2023," 2023. Accessed: Nov. 07, 2024. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/

[4] S. Romanosky and Z. Goldman, "Understanding Cyber Collateral Damage," *Journal of National Security Law & Policy*, vol. 9, no. 2, pp. 233–257, 2017.

[5] E. Waltz, *Information warfare: Principles and operations*. Boston: Artech House, 1998.

[6] Verizon, “Verizon Data Breach Investigations Report 2024,” 2024. Accessed: Nov. 07, 2024. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[7] A. Vittorio, “Merck’s $1.4 Billion Insurance Win Splits Cyber From ‘Act of War,’” *Bloomberg Law*, Jan. 19, 2022. Accessed: Nov. 07, 2024. [Online]. Available: https://news.bloomberglaw.com/privacy-and-data-security/mercks-1-4-billion-insurance-win-splits-cyber-from-act-of-war

[8] G. Corera, “Cyber-attack: US and UK blame North Korea for WannaCry,” *BBC News*, Dec. 19, 2017. Accessed: Nov. 07, 2024. [Online]. Available: https://www.bbc.com/news/world-us-canada-42407488

[9] J. P. Farwell and R. Rohozinski, “Stuxnet and the Future of Cyber War,” *Survival (Lond)*, vol. 53, no. 1, pp. 23–40, Feb. 2011, doi: 10.1080/00396338.2011.555586.

[10] M. Robinson, K. Jones, and H. Janicke, “Cyber warfare: Issues and challenges,” *Comput Secur*, vol. 49, pp. 70–94, Mar. 2015, doi: 10.1016/j.cose.2014.11.007.

[11] M. Schmitt, Ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2013.

[12] M. N. Schmitt, Ed., *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press, 2017.

[13] P. Pascucci, “Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution,” *Minnesota Journal of International Law*, vol. 26, pp. 419–460, 2017.

[14] N. Ebner, “IFAR2 Fact Sheet: Cyber Space, Cyber Attack and Cyber Weapons - A Contribution to the Terminology,” 2015.

[15] NATO, “Warsaw Summit Communiqué,” 2016. Accessed: Nov. 07, 2024. [Online]. Available: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

[16] NIST, “Special Publication NIST SP 800-160v1r1 Engineering Trustworthy Secure Systems,” 2022.

[17] H. Lin, “Offensive cyber operations and the use of force,” *Journal of National Security Law & Policy*, vol. 4, pp. 63–86, 2010.

[18] M. Smeets, “The Strategic Promise of Offensive Cyber Operations,” *Strategic Studies Quarterly*, vol. 12, no. 3, pp. 90–113, 2018.
[19] K. Huang, M. Siegel, and S. Madnick, “Systematically Understanding the Cyber Attack Business,” *ACM Comput Surv*, vol. 51, no. 4, pp. 1–36, Jul. 2019, doi: 10.1145/3199674.
[20] Microsoft, “Microsoft Digital Defense Report 2024,” 2024. Accessed: Oct. 29, 2024. [Online]. Available: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024
[21] J. A. Green, *Cyber Warfare*. Taylor & Francis, 2015.
[22] T. Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies*, vol. 35, no. 1, pp. 5–32, Feb. 2012, doi: 10.1080/01402390.2011.608939.
[23] T. Rid, “Why You Haven’t Heard About the Secret Cyberwar in Ukraine,” *New York Times*, Mar. 18, 2022. Accessed: Nov. 07, 2024. [Online]. Available: https://www.nytimes.com/2022/03/18/opinion/cyberwar-ukraine-russia.html
[24] M. G. Solomon and M. Chapple, *Information security illuminated*. Jones & Bartlett Publishers, 2004.
[25] J. R. Lindsay, “Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack,” *J Cybersecur*, vol. 1, no. 1, pp. 53–67, 2015.
[26] M. Libicki, *Cyberdeterrence and cyberwar*. RAND Corporation, 2009.
[27] M. Dunn Cavelty, *The Politics of Cyber-Security*. Taylor & Francis, 2025.
[28] L. Ablon and A. Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. RAND Corporation, 2017.
[29] K. Hausken and J. W. Welburn, “Attack and Defense Strategies in Cyber War Involving Production and Stockpiling of Zero-Day Cyber Exploits,” *Information Systems Frontiers*, vol. 23, no. 6, pp. 1609–1620, Dec. 2021, doi: 10.1007/s10796-020-10054-z.

[30] T. Herr, “PrEP: A Framework for Malware & Cyber Weapons,” *Journal of Information Warfare*, vol. 13, no. 1, pp. 87–106, 2014.
[31] W. Gragido and J. Pirc, “Seven Commonalities of Subversive Multivector Threats,” in *Cybercrime and Espionage*, Syngress, 2011.
[32] R. Ottis, “Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective,” Tallinn, Estonia, 2008.
[33] E. Bumiller and T. Shanker, “Panetta Warns of Dire Threat of Cyberattack on U.S.,” *New York Times*, Oct. 11, 2012.
[34] M. Libicki, “The Cyber War that Wasn’t,” in *Cyber War in Perspective: Russian Aggression against Ukraine*, K. Geers, Ed., Tallinn: NATO CCD COE Publications, 2015.
[35] Council on Foreign Relations, “Cyber Operations Tracker.” Accessed: Nov. 07, 2024. [Online]. Available: https://www.cfr.org/cyber-operations/
[36] J. Arquilla and D. Ronfeldt, “Cyberwar is coming!,” *Comparative Strategy*, vol. 12, no. 2, pp. 141–165, Apr. 1993, doi: 10.1080/01495939308402915.
[37] P. W. Dowd and J. T. McHenry, “Network security: it’s time to take it seriously,” *Computer (Long Beach Calif)*, vol. 31, no. 9, pp. 24–28, Sep. 1998.
[38] M. N. Schmitt, “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,” *Columbia Journal of Transnational Law*, vol. 37, p. 885, 1998.
[39] J. Adams, *The Next World War: Computer are the Weapons and the Front Line is Everywhere*. Simon & Schuster, 1998.
[40] N. Tsagourias and M. Farrell, “Cyber attribution: technical and legal approaches and challenges,” *European Journal of International Law*, vol. 31, no. 3, pp. 941–967, Aug. 2020.
[41] F. J. Egloff and M. Smeets, “Publicly attributing cyber attacks: a framework,” *Journal of Strategic Studies*, vol. 46, no. 3, pp. 502–533, Apr. 2023, doi: 10.1080/01402390.2021.1895117.
[42] D. Efrony and Y. Shany, “A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice,” *American Journal of International Law*, vol. 112, no. 4, pp. 583–657, Oct. 2018, doi: 10.1017/ajil.2018.86.

[43] D. E. Denning and B. J. Strawser, “Moral Cyber Weapons,” in *The Ethics of Information Warfare*, M. Taddeo and L. Floridi, Eds., Springer International Publishing, 2014, pp. 85–103.
[44] T. Rid and B. Buchanan, “Attributing Cyber Attacks,” *Journal of Strategic Studies*, vol. 38, no. 1–2, pp. 4–37, Jan. 2015, doi: 10.1080/01402390.2014.977382.
[45] K. Andersson *et al.*, “Military utility: A proposed concept to support decision-making,” *Technol Soc*, vol. 43, pp. 23–32, Nov. 2015.
[46] O. A. Hathaway *et al.*, “The Law of Cyber-Attack,” *Calif Law Rev*, vol. 100, no. 4, pp. 817–885, 2012.
[47] J. Sigholm, “Non-State Actors in Cyberspace Operations,” *Journal of Military Studies*, vol. 4, no. 1, pp. 1–37, Dec. 2013, doi: 10.1515/jms-2016-0184.
[48] K. Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon*. Crown Publishing, 2014.
[49] A. Greenberg, “The International Criminal Court Will Now Prosecute Cyberwar Crimes,” *Wired*, Sep. 07, 2023.
[50] C. von Clausewitz, *On War*. Princeton University Press, 1976.
[51] T. Brück, O. J. de Groot, and C. Bozzoli, “How Many Bucks in a Bang: On the Estimation of the Economic Costs of Conflict,” in *The Oxford Handbook of the Economics of Peace and Conflict*, M. R. Garfinkel and S. Skaperdas, Eds., Oxford University Press, 2012, ch. 12.
[52] G. Harris, “Estimates of the economic cost of armed conflict: The Iran-Iraq war and the Sri Lankan civil war,” in *The Economics of Conflict and Peace*, J. Brauer and W. G. Gissy, Eds., Routledge, 1997.
[53] European Union Military Committee, “Avoiding and Minimizing Collateral Damage in EU-led Military Operations Concept,” Brussels, 2016. Accessed: Jan. 30, 2024. [Online]. Available: https://data.consilium.europa.eu/doc/document/ST-5785-2016-INIT/en/pdf
[54] N. C. Rowe, “Distinctive Ethical Challenges of Cyberweapons,” in *Research Handbook on International Law and Cyberspace*, N. Tsagourias, Ed., Edward Elgar Publishing, 2015, ch. 14, pp. 307–325.

[55] A. H. Eden, “Three paradigms of computer science,” *Minds Mach (Dordr)*, vol. 17, no. 2, pp. 135–167, Jul. 2007, doi: 10.1007/s11023-007-9060-8.

[56] E. Larsson and J. Sigholm, “Dataset: Cyber incidents in the Ukrainian conflict 2013-2020.” Accessed: May 24, 2024. [Online]. Available: https://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-12386

[57] F. Almeida, “Strategies to perform a mixed methods study,” *European Journal of Education Studies*, vol. 5, no. 1, 2018.

[58] B. Kitchenham and P. Brereton, “A systematic review of systematic review process research in software engineering,” *Inf Softw Technol*, vol. 55, no. 12, pp. 2049–2075, Dec. 2013, doi: 10.1016/j.infsof.2013.07.010.

[59] M. Vaismoradi and S. Snelgrove, “Theme in Qualitative Content Analysis and Thematic Analysis,” *Forum Qual Soc Res*, vol. 20, no. 3, 2019.

[60] University of York Centre for Reviews and Dissemination, “What are the criteria for the inclusion of reviews on DARE?,” 2014. Accessed: Jan. 31, 2024. [Online]. Available: https://www.ncbi.nlm.nih.gov/books/NBK285222/

[61] A. S. Lee, “A Scientific Methodology for MIS Case Studies,” *MIS Quarterly*, vol. 13, no. 1, p. 33, Mar. 1989, doi: 10.2307/248698.

[62] S. Collins and S. McCombie, “Stuxnet: the emergence of a new cyber weapon and its implications,” *Journal of Policing, Intelligence and Counter Terrorism*, vol. 7, no. 1, pp. 80–91, Apr. 2012, doi: 10.1080/18335330.2012.653198.

[63] K. J. Boyte, “A Comparative Analysis of the Cyberattacks Against Estonia, the United States, and Ukraine: Exemplifying the Evolution of Internet-Supported Warfare,” *International Journal of Cyber Warfare and Terrorism*, vol. 7, no. 2, 2017.

[64] B. Valeriano, “Harvard Dataverse: Dyadic Cyber Incident Dataset v 2.0.” Accessed: Feb. 01, 2024. [Online]. Available: https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/CQOMYV

[65] S. Romanosky, “Examining the costs and causes of cyber incidents,” *J Cybersecur*, pp. 121–135, Aug. 2016, doi: 10.1093/cybsec/tyw001.

[66] Swedish Research Council, “Ethics in research and good research practice.” Accessed: Nov. 07, 2024. [Online]. Available: https://www.vr.se/english/mandates/ethics/ethics-in-research.html

[67] All European Academies (ALLEA), “The European Code of Conduct for Research Integrity, revised edition,” 2017. Accessed: Nov. 07, 2024. [Online]. Available: https://www.allea.org/wp-content/uploads/2017/05/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017.pdf

[68] H. Douglas, “Values in Science,” in *The Oxford Handbook of Philosophy of Science*, P. Humphreys, Ed., Oxford University Press, 2016.

[69] J. J. Randolph and R. Bednarik, “Publication Bias in the Computer Science Education Research Literature,” *Journal of Universal Computer Science*, vol. 14, no. 4, pp. 575–589, 2008.

[70] U.S. Air Force, “Air Force Doctrine Publication 3-60, Targeting,” 2021. Accessed: Feb. 01, 2024. [Online]. Available: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-60/3-60-AFDP-TARGETING.pdf

[71] A. Arnbak, H. Asghari, M. Van Eeten, and N. Van Eijk, “Security collapse in the HTTPS market,” *Commun ACM*, vol. 57, no. 10, pp. 47–55, Sep. 2014, doi: 10.1145/2660574.

Expanding the view on Offensive Cyber Operations

Society relies upon the internet, a globally interconnected collection of networked information systems. These systems often contain critical vulnerabilities, giving states and state-sponsored groups compelling reasons to act in and through cyberspace. While state-sponsored cyberattacks can be both permissible and effective, they commonly have unintended effects: cyber collateral damage. This thesis investigates the balance between the operational effects of cyber operations and their collateral costs; the cost/benefit dilemma of offensive cyber operations. It does so by considering the potential benefit of high-impact cyberattacks, e.g. supply chain vulnerability implantation, and by using econometric methods to calculate the cost of collateral damage engendered when cyberspace is used as a domain of warfare. The thesis further presents a bottom-up analysis which shows that the economic damage caused by cyberattacks in the Russo-Ukrainian conflict 2014-2021 to be an insignificant part of the Ukrainian GDP. Finally, the thesis argues that the full cost of attacks should be measured and included in models for collateral damage estimation. Such estimates should be included into national cyber doctrines to minimize unintended effects and ensure efficient and appropriate use of cyber capabilities.

ISBN 978-91-7867-572-2 (print)

ISBN 978-91-7867-573-9 (pdf)

ISSN 1403-8099

LICENTIATE THESIS | Karlstad University Studies | 2025:20